Threat Group Cards: A Threat Actor Encyclopedia

Archived: 2026-04-05 23:33:53 UTC

Tool: ToxicPanda

Names	ToxicPanda
Category	Malware
Type	Banking trojan, Backdoor
Description	(Cleafy) ToxicPanda belongs to the modern RAT generation of mobile malware, as its Remote Access capabilities allow Threat Actors (TAs) to conduct Account Takeover (ATO) directly from the infected device, thus exploiting the On Device Fraud (ODF) technique. This consolidation of this technique has already been seen by other banking trojans, such as Medusa, Copybara, and, recently, BingoMod. Adopting a manual approach has several advantages: it requires less skilled developers, TAs can distribute the malware's target base to any banking customers, and bypass various behavioral detection countermeasures put in place by multiple banks and financial services.
Information	<https://www.cleafy.com/cleafy-labs/toxicpanda-a-new-banking-trojan-from-asia-hit-europe-and-latam>
Malpedia	<https://malpedia.caad.fkie.fraunhofer.de/details/apk.toxic_panda>

Last change to this tool card: 27 December 2024

Download this tool card in JSON format

All groups using tool ToxicPanda

Changed	Name	Country	Observed	
Unknown groups				
	[Interesting malware not linked to an actor yet]			

1 group listed (0 APT, 0 other, 1 unknown)

Source: https://apt.etda.or.th/cgi-bin/listgroups.cgi?u=967382b3-4f2a-40d5-b0de-3542861b554b